

AMENDMENTS IN THE ABSTRACT

Please replace the present abstract with the following rewritten abstract:

A method and system for ensuring security-compliant creation and signing of endorsement keys of manufactured trusted platform modules. The endorsement keys are generated for the trusted platform module (TPM). The TPM vendor selects an N-byte secret and stores the N-type secret in the trusted platform module along with the endorsement keys. The secret number cannot be read outside of the trusted platform module. The secret number is also provided to the credential server of the original equipment manufacturer. During the endorsement key (EK) credential process, the trusted platform module generates an endorsement key, which comprises both the public key and a hash of the secret and the public key. The credential server matches the hash within the endorsement key with a second hash of the received public key (from the endorsement key) and the vendor provided secret. The EK certificate is generated and inserted into the trusted platform module only when a match is confirmed.